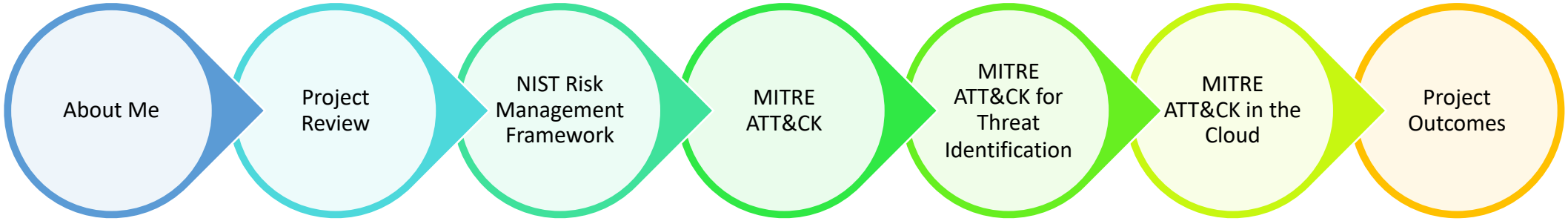
Improving NIH Cybersecurity Using MITRE ATT&CK

Jared Stancombe

Civic Digital Fellow, Coding It Forward

National Institutes of Health

Presentation Agenda



About Me

Cybersecurity Experience

- M.S. Cybersecurity Risk Management from Indiana University
- Former Incident Response Analyst, Indiana University
- Research with the NATO Cooperative Cyber Defence Centre of Excellence
- 2019 & 2020 Semifinalist, Atlantic Council Cyber 9/12 Strategy Challenge

Social Impact Work

- Global Health Corps Fellow, Action Africa Help International, Zambia
- William J. Clinton Fellow, American India Foundation
- AmeriCorps Member, City Year Washington, DC
- Board Member, United Way of South Central Indiana

Previous Government Experience

- Management and Program Analyst, DHS USCIS
- Program Officer, USAID DELIVER Project

Projects

Conduct research on how to apply MITRE ATT&CK in the NIST Risk Management Framework assessment and authorization process.

Write a wiki article on using MITRE ATT&CK for cloud service platforms.

Conduct a “Lunch and Learn” presentation with relevant NIH stakeholders on using MITRE ATT&CK to identify threats in Security Assessment Reports (SAR).

Why are these projects important?

MITRE ATT&CK is becoming the language of threat management within the cybersecurity community and NIH does not currently use it.

Current means of threat identification is a “paperwork exercise” and not based upon identifying areas of real risk, but instead used to check a box.

Identifying actual threats can inform how to better identify, detect, and mitigate against them.

NIH InfoSec is heavily siloed. MITRE ATT&CK can encourage inter-team collaboration to improve NIH cybersecurity maturity and efficacy.

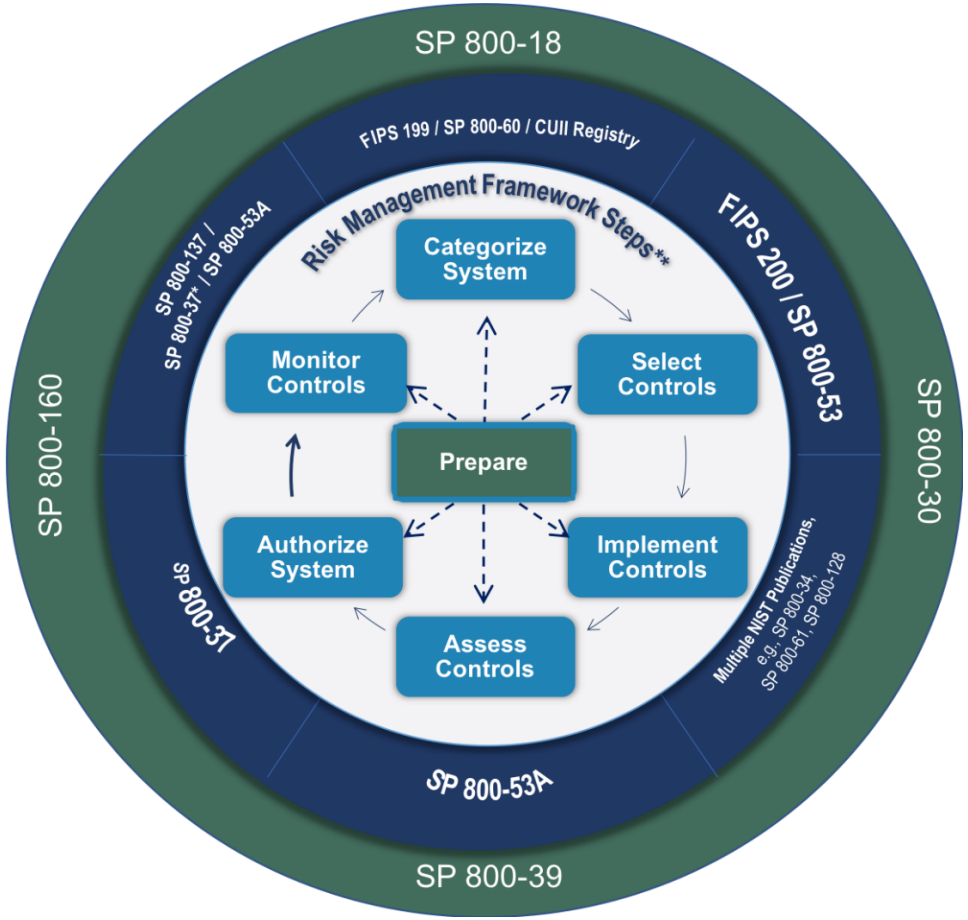
NIST RMF: Assessment & Authorization

Assess Controls

- Determines if the controls selected for implementation are:
  - implemented correctly
  - operating as intended
  - producing the ***desired outcome*** with respect to meeting the ***security and privacy requirements*** for the system and the organization

Authorize System

- Determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.

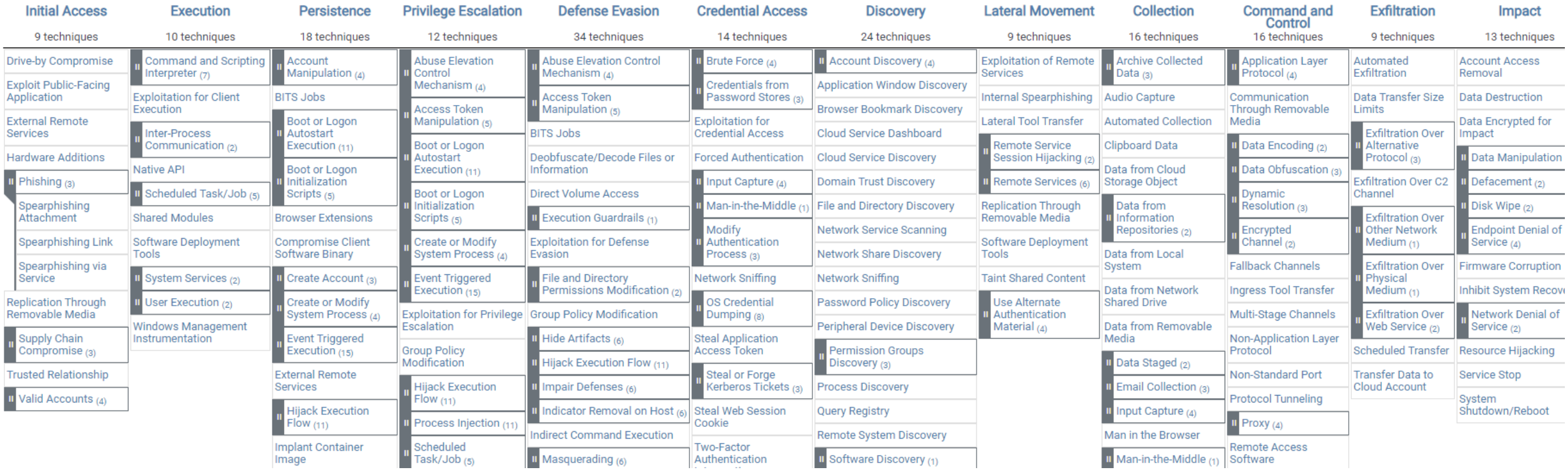


Threat Identification in Security Assessment Reports

- **Generic identification** of physical, environmental, & man-made threats
- **Generic categorization** of purposeful, unintentional, or environmental threat categories
- **Generic assessment** of threats & risks based upon potential impacts:
  - Modification of data
  - Data destruction
  - Unavailable accurate records
  - Denial of service
- **Compliance-oriented**

ID	Threat Name	Type Identifier	Description	Confidentiality	Integrity	Availability
T-1	Alteration	U, P, E	Alteration of data, files, or records.		Modification	
T-2	Audit Compromise	P	An unauthorized user gains access to the audit trail and could cause audit records to be deleted or modified, or prevents future audit records from being recorded, thus masking a security relevant event.		Modification or Destruction	Unavailable Accurate Records
T-3	Bomb	P	An intentional explosion.		Modification or Destruction	Denial of Service
T-4	Communications Failure	U, E	Cut of fiber optic lines, trees falling on telephone lines.			Denial of Service
T-5	Compromising Emanations	P	Eavesdropping can occur via electronic media directed against large scale electronic facilities that do not process classified National Security Information.	Disclosure		
T-6	Cyber Brute Force	P	Unauthorized user could gain access to the information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.	Disclosure	Modification or Destruction	Denial of Service
T-7	Data Disclosure Attack	P	An attacker uses techniques that could result in the disclosure of sensitive information by exploiting weaknesses in the design or configuration.	Disclosure		
T-8	Data Entry Error	U	Human inattention, lack of knowledge, and failure to cross-check system activities could contribute to errors becoming integrated and ingrained in automated systems.		Modification	

How can we improve the identification of threats to NIH systems?

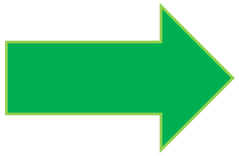


12 Tactics, 290+ Techniques, & Sub-Techniques

Comparing Threat Identification Methods

Simple Threat Identification

- **Generic identification** of physical, environmental, & man-made threats
- **Generic categorization** of purposeful, unintentional, or environmental threat categories
- **Generic assessment** of threats & risks based upon potential impacts:
  - Modification of data
  - Data destruction
  - Unavailable accurate records
  - Denial of service
- **Compliance-oriented**

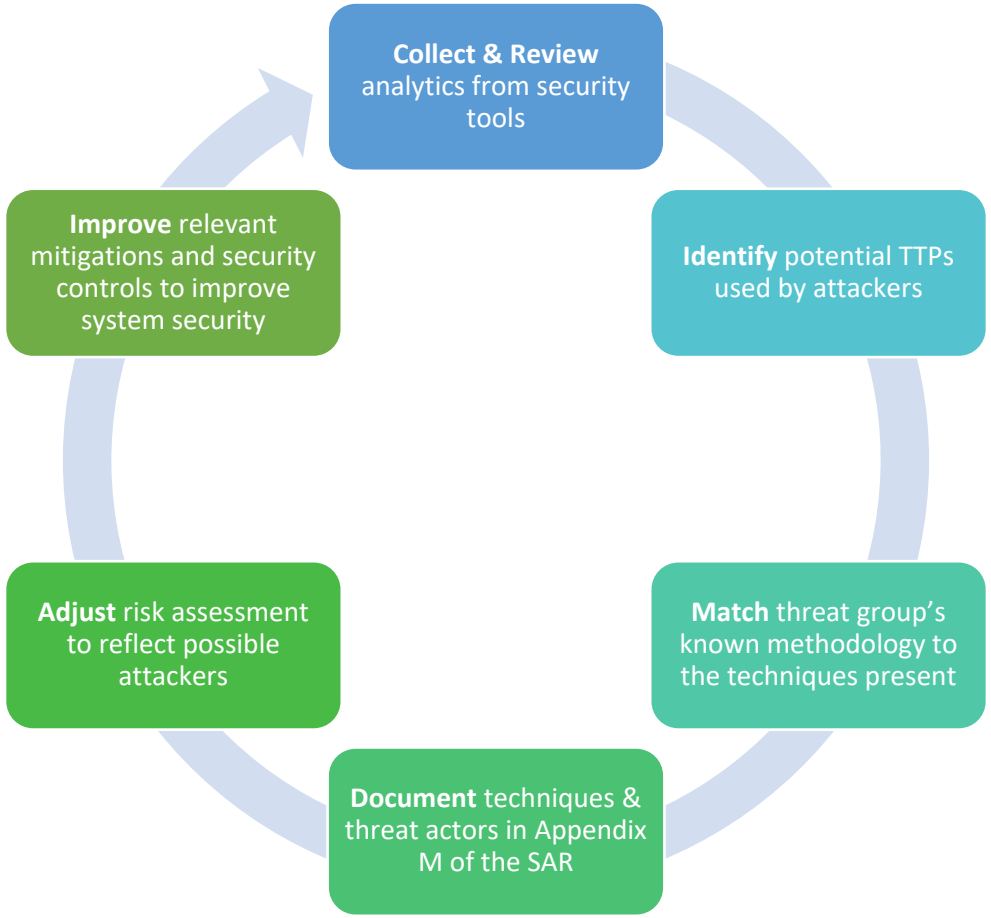


MITRE ATT&CK Cyber Threat Identification

- **Identification of specific threat actors** based upon real-world observations of tactics, techniques, & procedures (TTPs)
- Used to understand the **process** of a cyber attack, instead the end result
- **Map** threat actor TTPs through different stages of cyber attacks
- **Threat-oriented**
- **Actionable**

Using MITRE ATT&CK in Security Assessment Reports

- How can artifacts from penetration testing, vulnerability assessments, code reviews, tech support tickets, logs can be mapped to MITRE ATT&CK?
- How can these artifacts be mapped to MITRE ATT&CK tactics, techniques, and procedures (TTPs)?
- How can threats be identified using these TTPs?
- How does this change the assessment of risk to the system that was assessed?
- How can threats from these threat actors be identified and mitigated against?



Using MITRE ATT&CK in the Cloud

Analytics:

- Use security tools to create, collect, and analyze security analytics from sources such as AWS CloudTrail logs, Office365 audit logs, network device logs, and authentication logs
- Analytics can be collected using other methods such as monitoring processes on endpoints and how processes are using network resources

Detection and Mitigation:

- Identify common vectors of attack or indicators of compromise (IOCs)
- Identify how to detect and mitigate against attacks

Security Engineering:

- Identify gaps in security control coverage
- Make risk-informed decisions on security control deployment
- Improve efficiency of security control investments

Penetration Testing:

- Take results of penetration testing and vulnerability assessments and map them to MITRE ATT&CK to identify how to detect and mitigate against attacks
- Emulate adversary behaviors during penetration testing

Project Outcomes

Lunch & Learn Presentation

- Introduced MITRE ATT&CK to over 150 NIH stakeholders and taught them how to use MITRE ATT&CK in Security Assessment Reports
- Opened dialogue between the A&A team and other teams such as Threat Management and Incident Response (TMIR) on using MITRE ATT&CK
- Opened the door for the use of MITRE ATT&CK across NIH

Wiki Article

- Provides the first written internal resource that NIH Information Security stakeholders can reference on MITRE ATT&CK and its applications

A&A Team Experience

- Very supportive staff and supervisors who mentored me throughout the fellowship
- Supervisors also helped me navigate bureaucracy and understand how bureaucracy could impact my projects
- Meetings with staff across NIH InfoSec including the CIO
- Amazing team dynamics! Staff was incredibly supportive and accessible.
- Inspired me to apply to the TechCongress Innovation Scholars Program